DOI 10.5817/MUJLT2019-2-11

PROCEDURAL AND INSTITUTIONAL BACKING OF TRANSPARENCY IN ALGORITHMIC PROCESSING OF RIGHTS*

by

RADIM POLČÁK**

Efficient enforcement of legal substance requires proper procedures and capable institutions. In that respect, law is now being challenged by the emergence of automated systems that autonomously decide about matters concerning rights. The neuralgic point in enforcement of legal compliance of such systems, namely with regards to possible discrimination, is transparency. Currently, there exists, at least in the EU, particular individual right to know the logic of respective algorithms. The comment tries to narrow down the issue of actual enforceability of that right by investigating its basic procedural and institutional aspects.

KEY WORDS

Algorithmic State, Automated Decisions, Logic of Algorithms, Transparency of Algorithms

1. CONGRUENCE BETWEEN OFFICIAL ACTION AND DECLARED RULE

The last, and by far not the least important, of *Fuller's* principles of legality, is about congruence of substance and administration of rights, or of *"official action and declared rule"*[1]. All substantively grounded rights, however compliant with the earlier *Fuller's* principles, have no value if there are

* This comment is based on a research that was funded under the project C4E No. CZ.02.1.01/0.0/0.0/16_019/0000822. The author wishes to especially thank *Tomáš Sobek* who kindly provided inspiration for this comment thanks to his throughout knowledge of the work of late *Sir Terence Prachett*.

** radim.polcak@law.muni.cz, Head of the Institute of Law and Technology at the Faculty of Law, Masaryk University, The Czech Republic.

1 See Fuller, L. (1969) The Morality of Law. *Yale University Press*, p. 81.

no means available for their actual implementation. This principle of congruence of substance and procedure is being often materialised, amongst other places, at the *European Court of Human Rights* e.g. in cases when it takes too long for the courts in the member states to deliver justice.[2]

Besides cases of inability to deliver justice in reasonable time, there is a number of other possible cases of lack of congruence between substance and administration of rights. Despite these cases originate in hugely different domains, they all arise from disproportions between the law in books and the law in action which results in merely theoretical existence of respective rights. In all these cases, illegality (in *Fuller's* terms) arises from rights being just virtual but not actual.[3]

Following are two examples that illustrate the aforementioned virtuality of rights. These examples are in their natures very close to the below research questions, because they both relate to the role of state in getting complex information technologies under control.

The first example concerns data retention obligations that represent for more than a decade a mostly controversial issue across European jurisdictions.[4] Telecommunication operators have in some EU member states a duty to retain traffic data that are then available to law enforcement and security institutions. These obligations came under constitutional scrutiny across the EU and elsewhere namely because of concerns over privacy and personal data protection.

Regardless of whether traffic data are acquired by law enforcement upon data retention obligations or other procedural means, their availability represents a *conditio sine qua non* for prosecution of certain types of crimes.[5] Typically cyberstalking is quite impossible to prove without relevant traffic data that show statistics and technical details of actions of the perpetrator. If some jurisdiction would not allow access to traffic data,[6] cyberstalking would become a virtual crime in the sense that this crime would be only

---

[2] See for example Edel, F. (2007) *The length of civil and criminal proceedings in the case-law of the European Court of Human Rights.* Strasbourg: Council of Europe Publishing.

[3] For the meaning of "virtuality" and "actuality", see Lévy, P. (2002) *Becoming Virtual – Reality in the Digital Age.* Plenum Trade.

[4] See for example Boehm, F. and Cole, M. D. (2014) *Data Retention after the Judgement of the Court of Justice of the European Union.* EP Greens/EFA Group. Available online from: http://orbilu.uni.lu

[5] See for example a U.S. Congress. (2011) *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives.* U.S. Government Printing Office.

theoretically present in criminal statutes but would never actually appear in front of a court.

The second example is a case that involved *Google StreetView*. The *FCC* investigated an allegation that *Google* used an algorithm that was skimming the content, including highly sensitive personal data, from wireless networks in areas through which the *StreetView* cars were roaming.[7] *FCC* was only able to prove that *Google* cars were sniffing unsecured Wi-Fi networks, while there was lack of evidence that the same was done also to secured networks.[8] *Google* was at the end fined USD25,000 for what *David Kravets* named in *Wired* as *"stonewalling the investigation"*.[9]

The obstacles for which *Google* was fined were quite far from morally despicable. They can be simply explained as not enough willingness of *Google* to incriminate itself.

Google was asked to provide a copy of the actual data that it collected by sniffing wireless networks. In response, *Google* stated that

> *"it is not prudent or necessary for any governmental authority to examine the communications and personal information of U.S. citizens in order to resolve this matter"*.[10]

Put aside the question as to what extent it was "prudent and necessary" for *Google* to originally gather and process that data in the first place, what matters more is rather that the *FCC* was not given that data at all.

If, hypothetically, more pressure was put on *Google* by the *FCC*, *Google* could have e.g. given the *FCC* all the data collected by *StreetView* cars in raw format and asserted it possessed no means or motivation to interpret them. In that case, the *FCC* would have been left with an endless amount of binary data and a need to find someone to interpret them. A second option for

---

[6] It is to be noted here that some EU jurisdictions derogated the data retention duties, but traffic data are still available there through other procedural means (typically through general provisions related to stored communications). While there are some EU jurisdictions that do not provide for a duty to retain traffic data, there are no EU jurisdictions where traffic data would not be used by law enforcement.

[7] For analysis of this case, see Polcak, R. and Svantesson, D. (2017) *Information Sovereignty*. Edward Elgar Publishing, p. 170.

[8] See the FCC Notice of Apparent Liability for Forfeiture of 13 April 2012, File No EB-10-EH-4055. It is available in an unredacted version from: http://www.wired.com/images_blogs/threatlevel/2012/05/unredactedfccgoog.pdf

[9] See Kravets, D. (2012) An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle. *Wired*, 2 May. [online] Available from: https://www.wired.com/2012/05/google-wifi-fcc-investigation/ [Accessed 5 September 2019].

[10] See supra *FCC Notice*, fn. 89 (this footnote was for some reason blacked out in a redacted version that was later officially published by the *FCC*).

Google would be to assert that "the communications and personal information of U.S. citizens" had been deleted. The *FCC* would then either have to believe it or to prove that such a statement was not truthful which would require digging the respective data from somewhere. The second alternative is for obvious reasons rather unrealistic.[11]

Both above examples demonstrate clear disproportion between legislated and administered rights. First case shows a possible normative deficit when substantive provisions are not seconded with procedural rules needed for enforcement of respective substance. Second case shows actual practical (or institutional) deficit when procedural provisions do exist, but technical complexity of respective matter makes it impossible to efficiently use them and there is no way of normatively fixing it.

Lack of congruence between substance and administration of rights is hugely present also in algorithmic administration of rights.[12] The problem is relatively simple here – the lack of normative grounds, the amount and relevance of technical obstacles,[13] high costs, or all these factors at the same time,[14] prevent individuals as well as law enforcement from efficient review of legal compliance of respective algorithms.[15]

The growing importance of this issue even provoked the establishment of a research group within the *International Academy of Constitutional Law* titled *Algorithmic State, Society and Market – Constitutional Dimensions*. Its mission statement notes that

> *"[s]ince information and data are the new sources of power in the algorithmic society, patterns of market consolidation risk generating technological asymmetry which gravitates to a handful of multinational private players. The state then finds itself in a peculiar position, as it becomes partly dependent on the technologies of these players while vying*

[11] Lack of ability for a sovereign to exercise its powers is referred to in these regards by *Healey* as "cyber-Somalia". See Healey, J. (2011) The spectrum of National Responsibility for Cyberattacks. *The Brown Journal of World Affaires*, 18 (1), p. 63.

[12] The same issue is tackled from a different perspective in Pasquale, F. (2017) Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society. *Ohio State Law Journal*, 78, p. 1243.

[13] For other issues in legitimacy (or legality) of algorithmic administration of rights, see for example Gurumurthy, A. and Bharthur, D. (2018) Democracy and the Algorithmic Turn. *Sur – International Journal on Human Rights*, 27, p. 39.

[14] For a detailed analysis of problematic factors, see Bodo, B. et al. (2017) Tackling the Algorithmic Control Crisis – The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents. *Yale Journal of Law & Technology*, 19, p. 133.

[15] See Wolfe, A. (1990) Algorithmic Justice. *Cardozo Law Review*, 11, p. 1409.

> *for a similar position with respect to the data it collects and analyses, all at the same time as it retains the power (and legal responsibility) to regulate the industry and guarantee the protection of constitutional rights."*

Currently, there are two ways in which the law tries to normatively deal with this issue – either through transparency of algorithms or through compulsory human review of individual algorithmic decisions. Transparency aims at making algorithm as such reviewable in order to find our whether its code is in line with corresponding legal rules.[16] The right for a human review aims at individual confrontation of a resulting decision rendered by an algorithm with a human assessment. The difference between both these legal tools is that transparency covers congruence *in abstracto* while the right for human review lays down a congruence review *in concreto*.

This comment, that is also to accompany a research proposal to the aforementioned research group, primarily focuses on the congruence *in abstracto*, i.e. transparency of algorithms. In order to break this complex problem down, we further look at two of its mostly relevant elements: procedure and institutions. Our aim in this comment is not to resolve any of these two issues, but rather to identify their scope and name their neuralgic points. At first, we will briefly look at the right to know the logic of rights-administering algorithms and try to define the question as to *what* should that right mean in particular from procedural perspective. Secondly, we will formulate subsequent research question as to *who* should implement and enforce such procedure.

2. PROCEDURAL ISSUES IN COMPLIANCE REVIEW

The right to know the logic of algorithmic processing of rights is already laid down in some countries – e.g. in the EU it is legislated in Art. 12 in connection with Recital 63 of the GDPR. At first sight, this right seems to serve as a procedural norm that deals with the issue of transparency of algorithms and consequently with congruence between substance and administration of algorithmically processed rights.

However, the right to know the logic of algorithmic decisions does not actually represent a norm (or truly a "right") but rather only a general

[16] See Perel, M. and Elkin-Koren, N. (2017) Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, 69, p. 181.

principle. The scope of this right is so general that it is utterly impossible to directly (i.e. through syllogistic application upon particular facts) transform it into particular rights claimable by individuals who were affected by algorithmic decisions. In other words, if someone's loan application gets algorithmically rejected and the rejected applicant claims the right to know the logic of respective algorithm, there is no way to imply what exactly she is entitled to get.[17] If a court ruling would state e.g. that the plaintiff is "entitled to receive information on the logic of processing of her loan application", nobody (including the defendant) would be able to determine what should be done in order to comply.

One might understand the transparency right in the way that the applicant is entitled to receive just general information about factors that are taken into account by the algorithm. In that case, there is no way for the applicant or an independent reviewer to prove or even guess whether the algorithm works in line with substantive laws (e.g. with laws that ban discrimination).

Another possible interpretation is that the applicant is entitled to receive the actual code of the algorithm. In that case, which is not even overly probable due to legal constraints such as protection of copyrights or trade secrets, the applicant would be provided with an actual computer code and left to her own regarding its meanings – or provided with an explanation of the code that she will be never able to verify against the actual code.

Third option is that the applicant gets an opportunity to reversely engineer the algorithm in the way that the algorithm would be made available for testing of inputs and outputs. Such testing might then lead to a sort of recreation of the way in which the algorithm works. Similar to the previous case, finding out anything useful about the actual "logic of processing" is quite impossible here if the applicant is a common person and does not have behind her an army of boffins with a supercomputer technology.[18]

If we assume that the algorithm in question really lacks congruence with substantive rights, e.g. by being unreasonably discriminatory, a question remains as to how it is actually possible to reach particular legally relevant

[17] An attempt regarding clarification of this right is made in part dedicated to Art. 12 of the GDPR in Kuner, C. Bygrave, L. and Docksey, C. (2019) *The EU General Data Protection Regulation – A Commentary.* Oxford University Press, forthcoming.

[18] In addition, the availability of the algorithm for a reverse engineering would not give the investigator a proper picture in case of autonomous systems – see infra.

conclusion about such lack of congruence. The problem simply is that the transparency requirement is so general that it has no practical meaning in regular cases of complex or even autonomous algorithms.

3. INSTITUTIONAL ISSUES IN COMPLIANCE REVIEW

The issue of transparency seems a bit easier with man-made algorithms, because there possibly exists some "man" who ordered coding or even directly coded respective lack of congruence into the algorithm. Such person should then be able under existing legal procedures to state such lack of congruence in a legally relevant way (e.g. as a witness at court). However, the probability of that happening in real life is quite the same as it was with *Google* incriminating itself in the above Wi-Fi sniffing example.

Even worse from transparency perspective are cases when algorithms are made autonomously with no direct human involvement, i.e. in the case of neural networks or other AI-based systems that are only coded by humans to learn.[19] The resulting autonomously generated algorithm is in these cases unreadable even for an army of boffins. If such algorithm unreasonably discriminates or does anything similarly unlawful, it might be quite impossible even for its creator to find the core of the problem, not even speaking about repairing it.[20]

Both above reasons are good enough for assuming that any other than utterly simple algorithms need to be legally tackled either as black or nearly-black boxes.[21] While it is certainly possible to provide for normative requirements for turning black in this case into some shade of grey (such as those transparency requirements mentioned above), there still remains a question as to institutional backing of such arrangements.[22]

---

[19] See for example Lehr, D. and Ohm, P. (2017) Playing with the Data: What Legal Scholars Should Learn about Machine Learning. *University of California, Davis, Law Review*, 51, p. 653.

[20] A good example is the recent row over the *Tay* chatbot. Despite being developed by one of most advanced hi-tech corporations, *Microsoft*, *Tay* was constantly tweeting hate speech and nobody was able to fix that (so the only way for *Microsoft* to deal with all the shame was to simply switch *Tay* off). See Neff, G. and Nagz, P. (2016) Talking to Bots: Symbiotic Agency and the Case of Tay. *International Journal of Communication*, 10, p. 4915. The selection of most hateful autonomous tweets was published in Kleeman, S. (2016) Here Are the Microsoft Twitter Bot's Craziest Racist Rants. *gizmodo.com*, 24 March. [online] Available from: https://gizmodo.com/here-are-the-microsoft-twitter-bot-s-craziest-racist-ra-1766820160 [Accessed 5 September 2019].

[21] See for example Bose, U. (2015) The Black Box Solution of Autonomous Liability. *Washington University Law Review*, 92, p. 1325.

[22] The core role of institutional component of the rule of law represents a defining feature of institutional normativism. For a compendium of this methodological approach, see McCormick, N. and Weinberger, O. (1986) *An Institutional Theory of Law – New Approaches to Legal Positivism.* D Riedel Publishing.

In other words, one question is to provide for normative (or procedural) possibility of compliance review of algorithms, while the other issue is to have institutions pragmatically capable of doing so.[23]

One possible approach to the latter, institutional, issue is offered in the work of late *Sir Terence David John Pratchett*. His ant-powered computer[24] later named *Hex* also looks, even to its creator, *Ponder Stibbons*, as a black box, because calculations do not only depend here on man-made algorithms but mostly on behaviour of ants and, perhaps, also on complex informational effects of an anthill.[25] *Pratchett* paints here an institutional model where *Stibbons* is given the authority to declare that the *Hex* is faulty or broken and also the authority to adjust or repair it. That authority, however, is not based on the assumption that *Stibbons* precisely knows what is happening in the *Hex*, but because he is, thanks to his intelligence, experience, wisdom, moral profile and other personal properties, believed being capable of properly sensing that the results rendered by *Hex* are somewhat faulty.

The tricky element of this institutional arrangement is the required level of explicit reasoning for *Stibbons* to demonstrate a defect of the *Hex* as well as the required level of explanation of what and why *Stibbons* does in order to fix it. *Terry Prachett* puts it straight – *Stibbons'* thinking is so complex that it would not make sense for him to reason anything to anybody, because nobody would be able to understand him anyway.

It is obviously not possible to implement in full *Sir Terence's* model for identifying and fixing malfunctions in algorithmic processing of rights. One reason is that creators of respective systems do not always have to be as available and as capable as *Ponder Stibbons*. In addition, it is not entirely in line with rule of law principles to establish control or adjudicative competence only upon personal properties without at least a minimum requirement for knowing why, how and what is being done with the (allegedly) faulty machine.

At the same time, we already learned that relying purely on state--administered law enforcement is neither economically efficient nor

[23] See Baker, J. J. (2018) Beyond the Information Age: The Duty of Technology Competence in the Algorithmic Society. *South Carolina Law Review*, 69, p. 557.

[24] The first appearance of the *Hex* computer was in *Pratchett's* novel *Soul Music* from 1994.

[25] *Pratchett* does not mention that explicitly, but there is a good reason to believe that the *Hex* in fact uses fascinating complexity effects described by *Peter Coveney* and *Roger Highfield* in Coveney, P. and Highfield, R. (1996) *Frontiers of Complexity.* Penguin Random House, pp. 190–236.

technically possible in regulatory areas with strong technological aspect.[26] Consequently, we now witness a massive shift in technologically determined areas of law from state-administered behavioural rules to performance-based rules that are autonomously developed by those who are technically in charge (typically by service providers).[27] This move from state-ordered behaviour to state-ordered autonomous rulemaking has been already successfully applied in cybersecurity or personal data protection.[28]

In that sense, it is inevitable to allow the *Stibbons* regulatory model into areas such as algorithmic processing of rights not necessarily in its entirety, but at least in part. It means at first allowing and motivating an inclusion into the control and adjustment process also of those, who might not be officially legitimised, but whose technical competences and experience provide for reasonable and complex understanding of respective technology.

Also, it seems quite appropriate to admit that decisions about lack of legal compliance of algorithms will not always have to be based on perfect logical analysis and accordingly reasoned. That admittance is especially problematic, because one might say that code is a code and it ultimately breaks down to simple logical instructions as to turning I into O and *vice versa*. There is then no logical reason why a court or a similar body should be unable to come with exhausting logical argumentation as to what is wrong and how it should be fixed. The issue of *ipso facto* limited reviewability of decisions about lack of congruence of algorithms and laws is therefore highly problematic.[29]

---

[26] See Polcak, R. and Svantesson, D. (2017) *Information Sovereignty.* Edward Elgar Publishing, p. 6.

[27] For an explanation of nature and functioning of performance-based rules, see for example Coglianese, C. (2017) The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 50 (3), p. 525.

[28] Statutory examples include the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) or Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

[29] Similar in nature are recent cases of security concerns over certain telecommunication technologies – these concerns are often well grounded, but it is impossible for security authorities to directly point to a particular threatening line of code or to a particular chip. Media then tend to interpret these situations as allegations with no particular evidence.

4. CONCLUSIONS

This comment looked at congruence between substance and administration of algorithmically processed rights. It particularly focused on procedural and institutional backing of assessment of compliance of algorithms with applicable laws. The purpose of this comment was to identify particular assignments for comparative constitutional research in this field.

The first identified research assignment is based on the assumption that transparency requirement regarding algorithms is so broad that it covers everything and nothing at the same time, so there is a need to formulate at least a bit more particular procedural right (or rights). If such right or rights are found and formulated, they may be used either directly by being implemented into the black-letter law, codes of conduct etc. or indirectly through interpretation of the existing vastly general transparency requirements (such as those laid down currently in the GDPR) by courts or other public authorities.

Second particular research task that was identified in this comment relates to the extent to which particular legal systems are able to swallow a possible shift from recent standards of input and output legitimacy[30] of authoritative decisions[31] in order to provide for efficiency of abstract review of algorithms that administer rights. This task assumes that courts and other legitimised authorities are incapable of properly reviewing complex algorithms.

Even if a technically capable body is found or established, it might not be possible in regular cases to logically reason why some complex (or even autonomous) algorithm is not in line with rules that it is to administer. Consequently, there is a need to tackle the challenge of a required level of reasoning of legally relevant statements (mostly judgments, administrative decisions, official statements etc.) that declare lack of congruence between an algorithm and applicable law.

---

[30] For the meaning of the terms "input-" and "output legitimacy", see for example Loth, M. A. (2007) Courts in Search of Legitimacy: The Case of Wrongful Life. In: Sellers, M. (ed.). *Autonomy in the Law.* Springer Netherlands, pp. 73–96.

[31] For a comprehensive comparative study of such standards in the US and Europe, see De Lasser, M. (2009) *Judicial deliberations: a comparative analysis of transparency and legitimacy*. Oxford University Press.

LIST OF REFERENCES

[1] Baker, J. J. (2018) Beyond the Information Age: The Duty of Technology Competence in the Algorithmic Society. *South Carolina Law Review*, 69.

[2] Bodo, B. et al. (2017) Tackling the Algorithmic Control Crisis – The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents. *Yale Journal of Law & Technology*, 19.

[3] Boehm, F. and Cole, M. D. (2014) *Data Retention after the Judgement of the Court of Justice of the European Union.* EP Greens/EFA Group. Available online from: http://orbilu.uni.lu

[4] Bose, U. (2015) The Black Box Solution of Autonomous Liability. *Washington University Law Review*, 92.

[5] Coglianese, C. (2017) The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*, 50 (3).

[6] Coveney, P. and Highfield, R. (1996) *Frontiers of Complexity.* Penguin Random House.

[7] De Lasser, M. (2009) *Judicial deliberations: a comparative analysis of transparency and legitimacy*. Oxford University Press.

[8] Edel, F. (2007) *The length of civil and criminal proceedings in the case-law of the European Court of Human Rights.* Strasbourg: Council of Europe Publishing.

[9] Fuller, L. (1969) The Morality of Law. *Yale University Press*.

[10] Gurumurthy, A. and Bharthur, D. (2018) Democracy and the Algorithmic Turn. *Sur – International Journal on Human Rights*, 27.

[11] Healey, J. (2011) The spectrum of National Responsibility for Cyberattacks. *The Brown Journal of World Affairs*, 18 (1).

[12] Kleeman, S. (2016) Here Are the Microsoft Twitter Bot's Craziest Racist Rants. *gizmodo.com*, 24 March. [online] Available from: https://gizmodo.com/here-are-the-microsoft-twitter-bot-s-craziest-racist-ra-1766820160 [Accessed 5 September 2019].

[13] Kravets, D. (2012) An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle. *Wired*, 2 May. [online] Available from: https://www.wired.com/2012/05/google-wifi-fcc-investigation/ [Accessed 5 September 2019].

[14] Kuner, C. Bygrave, L. and Docksey, C. (2019) *The EU General Data Protection Regulation – A Commentary.* Oxford University Press, forthcoming.

[15] Lehr, D. and Ohm, P. (2017) Playing with the Data: What Legal Scholars Should Learn about Machine Learning. *University of California, Davis, Law Review*, 51.

[16] Lévy, P. (2002) *Becoming Virtual – Reality in the Digital Age.* Plenum Trade.

[17] Loth, M. A. (2007) Courts in Search of Legitimacy: The Case of Wrongful Life. In: Sellers, M. (ed.). *Autonomy in the Law.* Amsterdam: Springer Netherlands.

[18] McCormick, N. and Weinberger, O. (1986) *An Institutional Theory of Law – New Approaches to Legal Positivism.* D Riedel Publishing.

[19] Neff, G. and Nagz, P. (2016) Talking to Bots: Symbiotic Agency and the Case of Tay. *International Journal of Communication*, 10.

[20] Pasquale, F. (2017) Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society. *Ohio State Law Journal*, 78.

[21] Perel, M. and Elkin-Koren, N. (2017) Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, 69.

[22] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty.* Edward Elgar Publishing.

[23] U.S. Congress. (2011) *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives.* U.S. Government Printing Office.

[24] Wolfe, A. (1990) Algorithmic Justice. *Cardozo Law Review*, 11.